Образовательное частное учреждение
Дополнительного профессионального образования «Центр компьютерного обучения «Специалист» Учебно-научного центра при МГТУ им. Н.Э. Баумана»
(ОЧУ «Специалист»)

123242, город Москва, улица Зоологическая, дом 11, строение 2, помещение I, комната 11
ИНН 7701257303, ОГРН 1037739408189

Утверждаю:
Директор ОЧУ «Специалист»

_____/Т.С.Григорьева/
«01» июня 2018 года

Дополнительная профессиональная программа повышения квалификации

«IINS 3.0: Внедрение безопасности в сетях CISCO. Версия 3.0»

город Москва

Программа разработана в соответствии с приказом Министерства образования и науки Российской Федерации от 1 июля 2013 г. N 499 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам".

Повышение квалификации слушателей, осуществляемое в соответствии с программой, проводится с использованием модульного принципа построения учебного плана с применением различных образовательных технологий, в том числе дистанционных образовательных технологий и электронного обучения в соответствии с законодательством об образовании.

Дополнительная профессиональная программа повышения квалификации, разработана образовательной организацией в соответствии с законодательством Российской Федерации, включает все модули, указанные в учебном плане.

Содержание оценочных и методических материалов определяется образовательной организацией самостоятельно с учетом положений законодательства об образовании Российской Федерации.

Структура дополнительной профессиональной программы соответствует требованиям Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам, утвержденного приказом Минобрнауки России от 1 июля 2013 г. N 499.

Объем дополнительной профессиональной программы вне зависимости от применяемых образовательных технологий, должен быть не менее 16 академических часов. Сроки ее освоения определяются образовательной организацией самостоятельно.

Формы обучения слушателей (очная, очно-заочная, заочная) определяются образовательной организацией самостоятельно.

К освоению дополнительных профессиональных программ допускаются:

- лица, имеющие среднее профессиональное и (или) высшее образование;
- лица, получающие среднее профессиональное и (или) высшее образование.

Для определения структуры дополнительной профессиональной программы и трудоемкости ее освоения может применяться система зачетных единиц. Количество зачетных единиц по дополнительной профессиональной программе устанавливается организацией.

Образовательная деятельность слушателей предусматривает следующие виды учебных занятий и учебных работ: лекции, практические и семинарские занятия, лабораторные работы, круглые столы, мастер-классы, мастерские, деловые игры, ролевые игры, тренинги, семинары по обмену опытом, выездные занятия, консультации, выполнение аттестационной, дипломной, проектной работы и другие виды учебных занятий и учебных работ, определенные учебным планом.

Аннотация. Курс IINS 3.0 – 5-дневный курс под руководством инструктора, специально разработанный для того, чтобы предоставить слушателям начальные знания по обеспечению безопасности на коммутаторах и маршрутизаторах Cisco, а также межсетевых экранах CISCO ASA. Курс предназначен для инженеров и администраторов, занимающихся вопросами сетевой безопасности. В задачи, освещаемые курсом, входит разработка политики сетевой безопасности, работа с типовыми угрозами, защита и оценка активов и рисков, настройка оборудования, управление встроенными в Cisco IOS настройками безопасности, конфигурирование Zone-based firewall, настройка VPN (site-to-site, IPSec), знакомство с семейством Cisco ASA, с новым IPS – CISCO FIREPOWER. Данный курс - первый и самый нужный для изучения направления Security. Большая часть курса состоит из практических заданий, позволяющих применить полученные знания и умения в тестовой лабораторной сети. Технический контент курса был обновлен и адаптирован под Cisco IOS Software Release 15. Курс предназначен для сетевых инженеров, сотрудников технических служб, а также специалистов, которые занимаются

безопасностью сетей, профессионалов, которые хотят повысить свой уровень в области сетевой безопасности, архитекторов корпоративных сетей и сетей сервис-провайдеров.

Цель программы:

Цель курса - предоставить слушателям начальные знания по обеспечению безопасности на коммутаторах и маршрутизаторах Cisco, а также межсетевых экранах CISCO ASA.

Совершенствуемые компетенции

№	Компетенция	Направление подготовки
		ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ОБРАЗОВАНИЯ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ (УРОВЕНЬ БАКАЛАВРИАТА)
		Код компетенции
1	способностью проводить выбор исходных данных для проектирования	ПК-4
2	способностью использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований	ПК-25

Совершенствуемые компетенции в соответствии с трудовыми фикциями профессионального стандарта «Системный администратор информационно-коммуникационных систем" (Приказ Министерства труда и социальной защиты РФ от 5 октября 2015 г. N 684н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем").

№	Компетенция ОТФ	Направление подготовки
		ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ «Системный администратор информационно-коммуникационных систем»
		Трудовые функции (код)
1	B5 Администрирование прикладного программного Обеспечения инфокоммуникационной системы организации	B/01.5 Установка прикладного программного обеспечения B/02.5 Оценка критичности возникновения инцидентов при работе прикладного программного обеспечения. B/03.5 Оптимизация функционирования прикладного программного обеспечения B/04.5 Интеграция прикладного

		программного обеспечения в единую структуру инфокоммуникационной системы. B/05.5 Реализация регламентов обеспечения информационной безопасности прикладного программного обеспечения. B/06.5 Разработка нормативно-технической документации на процедуры управления прикладным программным обеспечением. B/07.5 Разработка требований к аппаратному обеспечению и поддерживающей инфраструктуре для эффективного функционирования прикладного программного обеспечения.

Планируемый результат обучения:

После окончания обучения Слушатель будет знать:

- Обеспечение безопасности на коммутаторах и маршрутизаторах Cisco, а также межсетевых экранах CISCO ASA.
- Разработка политики сетевой безопасности, работа с типовыми угрозами, защита и оценка активов и рисков, настройка оборудования, управление встроенными в Cisco IOS настройками безопасности.
- Конфигурирование Zone-based firewall, настройка VPN (site-to-site, IPSec), знакомство с семейством Cisco ASA, с новым IPS – CISCO FIREPOWER.

После окончания обучения Слушатель будет уметь:

- Описывать концепции сетевой безопасности
- Защищать сетевые устройства
- Внедрять механизмы сетевой безопасности на уровне 2 модели OSI
- Внедрять механизмы сетевой безопасности с помощью межсетевых экранов
- Внедрять VPN-технологии
- Описывать современные технологии и архитектуры безопасности

Учебный план:

Категория слушателей: Курс предназначен для сетевых инженеров, сотрудников технических служб, а также специалистов, которые занимаются безопасностью сетей, профессионалов, которые хотят повысить свой уровень в области сетевой безопасности, архитекторов корпоративных сетей и сетей сервис-провайдеров.

Требования к предварительной подготовке: Успешное окончание курса ICND2: Использование сетевого оборудования Cisco v 3.0 Часть 2 Официальный учебник + перевод руководства по лабораторным работам! или эквивалентная подготовка. «Английский язык. Уровень 2. Elementary, часть 2», или эквивалентная подготовка.

Срок обучения: 40 академических часов, в том числе 40 аудиторных, 0 самостоятельно (СРС).

Форма обучения: очная, очно-заочная, заочная. По желанию слушателя форма обучения может быть изменена и/или дополнена.

Режим занятий: дневной, вечерний, группы выходного дня.

№ п/п	Наименование модулей по программе	Общая трудоемкость (акад. часов)	Всего ауд. ч	В том числе		СРС,ч	Форма ПА[1]
				Лекций	Практ занятий		
1	Модуль 1. Введение в информационную безопасность	6	6	2	4	0	Лабораторная работа
2	Модуль 2. Обеспечение безопасности сетевых устройств	7	7	2	5	0	Лабораторная работа
3	Модуль 3. Безопасность канального уровня	7	7	2	5	0	Лабораторная работа
4	Модуль 4. Межсетевые экраны	7	7	2	5	0	Лабораторная работа
5	Модуль 5. VPN	7	7	2	5	0	Лабораторная работа
6	Модуль 6. Дополнительные технологии безопасности	6	6	2	4	0	Лабораторная работа
	Итого:	40	40	14	26	0	
	Итоговая аттестация	тестирование					

Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

Количество аудиторных занятий при очно-заочной форме обучения составляет 20-25% от общего количества часов.

Форма Промежуточной аттестации – см. в ЛНА «Положение о проведении промежуточной аттестации слушателей и осуществлении текущего контроля их успеваемости» п.3.3.

[1] ПА – промежуточная аттестация.

1. Календарный учебный график

Календарный учебный график формируется при осуществлении обучения в течение всего календарного года. По мере набора групп слушателей по программе составляется календарный график, учитывающий объемы лекций, практики, самоподготовки, выезды на объекты.

Неделя обучения	1	2	3	4	5	6	7	Итого часов
	пн	вт	ср	чт	пт	сб	вс	
1 неделя	4	4	4	4	4	-	-	20
СРС	0	0	0	0	0	-	-	0
2 неделя	4	4	4	4	4 ИА	-	-	20
СРС	0	0	0	0	0	-	-	0
Итого:	8	8	8	8	8	-	-	40
Примечание: ИА – Итоговая аттестация (тестирование)								

2. Рабочие программы учебных предметов

Модуль 1. Введение в информационную безопасность
Цель: описание концепции информационной безопасности «control plane» и «management plane»

Урок 1: Модель угроз

Цель: описание модели угроз

Рассматриваемые вопросы:

- Описание модели угроз
- DoS и DDoS
- Подмена трафика
- Атаки отражения и усиления
- Социальная инженерия
- Phishing
- Подбор паролей
- Атаки разведки
- Атаки переполнения буфера
- Атаки «человек-посредине»
- Malware
- Векторы потери данных
- Хакерские механизмы
- Прочее

Урок 2: Технологии защиты от угроз

Цель: описание технологий защиты от угроз

Рассматриваемые вопросы:

- Межсетевые экраны
- Системы предупреждения вторжений

- Безопасность содержимого
- VPN
- Безопасность конечных устройств
- Журналирование

Урок 3: Политика безопасности и базовые архитектурные принципы информационной безопасности

Цель: описание политики безопасности и базовых архитектурных принципов информационной безопасности

Рассматриваемые вопросы:

- Обзор информационной безопасности
- Классификация активов, уязвимостей и противомер
- Управление рисками
- Соответствие регуляторным требованиям
- Принципы дизайна безопасности
- Политика безопасности
- Зоны безопасности
- Функциональные элементы сети

Урок 4: Технологии криптографии

Цель: описание криптографических технологий

Рассматриваемые вопросы:

- Обзор криптографии
- Хэш-алгоритмы
- Шифрование
- Криптоанализ
- Алгоритмы симметричного шифрования
- Алгоритмы ассиметричного шифрования
- Протокол SSH
- Цифровые сигнатуры
- Обзор PKI
- Операции PKI
- Протокол SSL/TLS
- Управление ключами

Модуль 2. Обеспечение безопасности сетевых устройств
Цель: обеспечение безопасности «control plane» и «management plane» сетевых устройств

Урок 1: Внедрение AAA

Цель: конфигурация AAA на сетевых устройствах CISCO

Рассматриваемые вопросы:

- Знакомство с AAA
- Базы данных AAA
- Протоколы AAA
- Сервера AAA
- Конфигурация и работа SSH на IOS
- Авторизация на IOS по уровням привилегий
- Внедрение локальной аутентификации и авторизации AAA
- Авторизация с использованием ролевого разделения доступа к CLI
- TACACS+ на IOS

Урок 2: протоколы и системы управления

Цель: внедрение безопасного управления CISCO IOS и CISCO ASA

Рассматриваемые вопросы:

- Файловая система IOS
- Копирование файлов на и с устройств
- Проверка образа CISCO IOS по MD5
- Цифровые подписи на образах
- Отказоустойчивость образа IOS
- NTP
- Syslog
- Оповещения о превышении использования памяти и CPU
- Netflow
- Возможности управления устройством
- Конфигурация и работа HTTPS
- Конфигурация и работа SNMPv3
- Защита управления с помощью ACL
- Что нужно знать о паролях?

Урок 3: Защита «control plane»

Цель: Обзор защиты «control plane»

Рассматриваемые вопросы:

- Что такое «control plane»?
- CoPP (Control Plan Policing)
- CPPr (Control Plane Protection)
- Аутентификация протоколов маршрутизации
- Аутентификация маршрутов OSPF
- Аутентификация маршрутов EIGRP

Модуль 3. Безопасность канального уровня
Цель: внедрение безопасности «control plane» и «data plane» на коммутаторах

Урок 1: Безопасность инфраструктуры уровня 2

Цель: внедрение безопасности коммутирующей инфраструктуры

Рассматриваемые вопросы:

- Введение в безопасность уровня 2
- Коммутация Ethernet
- Обзор VLAN
- Конфигурация VLAN
- Транки 802.1Q
- Атаки на транки
- Конфигурация транков и защита их
- CDP
- Использование ACL
- ACL на коммутаторах
- Защита CAM
- Port Security
- PVLAN
- PVLAN Edge
- Атаки на PVLAN и защита от них

Урок 2: Безопасность протоколов уровня 2

Цель: внедрение безопасности протоколов уровня 2

Рассматриваемые вопросы:

- Обзор STP
- Атаки STP
- Противодействие атакам STP
- Обзор DHCP
- Атаки DHCP
- DHCP Snooping
- Обзор ARP
- Атака отравлением кэша ARP
- DAI

Модуль 4. Межсетевые экраны
Цель: Описание межсетевых экранов

Урок 1: Технологии межсетевых экранов

Цель: описание технологий межсетевых экранов

Рассматриваемые вопросы:

- Обзор межсетевых экранов
- Пакетные фильтры
- Межсетевые экраны с контролем соединений
- Прокси-сервера
- Межсетевые экраны нового поколения
- Журналирование

Урок 2: Знакомство с CISCO ASA 9.2

Цель: начальное конфигурирование CISCO ASA 9.2

Рассматриваемые вопросы:

- Семейство межсетевых экранов CISCO ASA
- Основные характеристики CISCO ASA
- Способы использования
- Контексты
- Отказоустойчивость
- Настройка доступа на CISCO ASA
- Настройка интерфейсов на CISCO ASA
- Обзор NAT
- Настройка NAT на CISCO ASA
- Настройка статического NAT на CISCO ASA
- Настройка динамического NAT на CISCO ASA
- Настройка PAT на CISCO ASA
- Настройка Policy PAT на CISCO ASA
- Проверка NAT

Урок 3: Контроль доступа и сервисные политики на CISCO ASA

Цель: обзор и конфигурация контроля доступа и сервисных политик на CISCO ASA

Рассматриваемые вопросы:

- Обзор правил обработки трафика на интерфейсах
- Конфигурация правил обработки трафика на интерфейсах
- Объектные группы
- Введение в CISCO ASA MPF
- Настройка CISCO ASA MPF

Урок 4: Зональный межсетевой экран CISCO IOS ZBF

Цель: описание и конфигурирование CISCO IOS ZBF

Рассматриваемые вопросы:

- Обзор технологии ZBF
- Зоны и зональные пары
- Описание C3PL
- Взаимодействие зон по умолчанию
- Настройка ZBF Class-map
- Настройка ZBF Policy-map

Модуль 5. VPN
Цель: Описание и конфиурирование VPN

Урок 1: Технологии IPSec

Цель: описание технологии IPSec

Рассматриваемые вопросы:

- IPSec VPN
- Сервисы IPSec
- Модель IPSec
- IKE
- IKE фаза 1
- Конфигурация ISAKMP
- Протоколы IPSEC
- IKE фаза 2
- Конфигурация IPSEC
- Криптографический стандарт «SUITE B»
- IKE версия 2
- IPSec и IPv6

Урок 2: Site-to-site VPN

Цель: конфигурирование Site-to-site VPN

Рассматриваемые вопросы:

- Туннели site-to-site
- Настройка туннеля site-to-site с помощью IPSec
- Шаг 1. Проверка совместимости ACL с IPSec
- Шаг 2. Настройка IKE фазы 1
- Шаг 3. Настройка IKE фазы 2 – наборы преобразований трафика
- Шаг 4. Настройка IKE фазы 2 – ACL для отбора трафика
- Шаг 5. Настройка IKE фазы 2 – крипто карты
- Проверка конфигурации IPSec
- Настройка Site-to-Site VPN на CISCO ASA
- Контроль настройки Site-to-Site VPN с помощью ASDM

Урок 3: VPN удаленного доступа

Цель: внедрение технологии VPN для удаленного доступа

Рассматриваемые вопросы:

- SSL и TLS
- Базовый Cisco AnyConnect SSL VPN
- Компоненты решения Cisco AnyConnect SSL VPN
- Аутентификация SSL VPN сервера
- Аутентификация SSL VPN клиента
- Назначение IP-адреса SSL VPN клиенту
- Настройка AnyConnect SSL VPN

Урок 4: Безклиентский VPN удаленного доступа

Цель: внедрение безклиентского VPN удаленного доступа

Рассматриваемые вопросы:

- Cisco Clientless SSL VPN
- Использование Cisco Clientless SSL VPN
- Методы доступа к ресурсам Cisco Clientless SSL VPN
- Базовое решение Clientless SSL VPN
- Аутентификация сервера в Basic Clientless SSL VPN
- Аутентификация клиентов в Basic Clientless SSL VPN
- Списки URL в Clientless SSL VPN
- Управление доступом в Clientless SSL VPN
- Конфигурирование Clientless SSL VPN

Модуль 6. Дополнительные технологии безопасности
Цель: обзор дополнительных технологий безопасности

Урок 1: Обнаружение и предупреждение вторжений

Цель: описание IDS и IPS систем

Рассматриваемые вопросы:

- Введение в IPS
- Терминология IPS
- Техники ухода от обнаружения и меры противодействия им
- Защита сети с помощью FIRESIGHT
- Защита FIRESIGHT до атаки
- Защита FIRESIGHT во время атаки
- Защита FIRESIGHT после атаки
- Вариаты внедрения FIRESIGHT
- Режимы «inline» и «Passive Mode»

Урок 2: Защита конечных систем

Цель: описание защиты конечных систем

Рассматриваемые вопросы:

- Обзор безопасности конечных систем
- Персональные межсетевые экраны
- Антивирусы и анти-spyware
- Централизованное управление политикой
- CISCO AMP для конечных систем

Урок 3: Безопасность контента

Цель: описание вопросов безопасности контента

Рассматриваемые вопросы:

- Внедрение CISCO ESA
- Обзор CISCO ESA

- Функциональные характеристики CISCO ESA
- Управление CISCO ESA
- Обработка почты с помощью CISCO ESA
- Внедрение CISCO WSA
- Обзор CISCO WSA
- Функциональные характеристики CISCO WSA
- Управление CISCO WSA
- Внедрение CISCO CWS
- Обзор CISCO CWS
- Функциональные характеристики CISCO CWS

Урок 4: Расширенные архитектуры безопасности

Цель: обзор дополнительных архитектур безопасности

Рассматриваемые вопросы:

- Модульный подход в безопасности
- Проблемы безопасности в современных сетях
- Управление идентификацией субъекта
- BYOD
- CISCO TRUSTSEC

4. Организационно-педагогические условия

Соблюдение требований к кадровым условиям реализации дополнительной профессиональной программы:

а) преподавательский состав образовательной организации, обеспечивающий образовательный процесс, обладает высшим образованием и стажем преподавания по изучаемой тематике не менее 1 года и (или) практической работы в областях знаний, предусмотренных модулями программы, не менее 3 (трех) лет;

б) образовательной организацией наряду с традиционными лекционно-семинарскими занятиями применяются современные эффективные методики преподавания с применением интерактивных форм обучения, аудиовизуальных средств, информационно-телекоммуникационных ресурсов и наглядных учебных пособий.

Соблюдение требований к материально-техническому и учебно-методическому обеспечению дополнительной профессиональной программы:

а) образовательная организация располагает необходимой материально-технической базой, включая современные аудитории, библиотеку, аудиовизуальные средства обучения, мультимедийную аппаратуру, оргтехнику, копировальные аппараты. Материальная база соответствует санитарным и техническим нормам и правилам и обеспечивает проведение всех видов практической и дисциплинарной подготовки слушателей, предусмотренных учебным планом реализуемой дополнительной профессиональной программы.

б) в случае применения электронного обучения, дистанционных образовательных технологий каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к электронной информационно-образовательной среде, содержащей все электронные образовательные ресурсы, перечисленные в модулях дополнительной профессиональной программы.

5. Формы аттестации и оценочные материалы

Образовательная организация несет ответственность за качество подготовки слушателей и реализацию дополнительной профессиональной программы в полном объеме в соответствии с учебным планом.

Оценка качества освоения дополнительной профессиональной программы слушателей включает текущий контроль успеваемости и итоговую аттестацию.

Промежуточная аттестация по данному курсу проводится в форме выполнения практических работ, к итоговой аттестации допускаются слушатели, выполнившие все практические работы.

Результаты итоговой аттестации слушателей ДПП в соответствии с формой итоговой аттестации, установленной учебным планом, выставляются по двух бальной шкале («зачтено\незачтено»).

Слушателям, успешно освоившим дополнительную профессиональную программу и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации.

Слушателям, не прошедшим итоговой аттестации или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть дополнительной профессиональной программы и (или) отчисленным из образовательной организации, выдается справка об обучении или о периоде обучения по образцу, самостоятельно устанавливаемому образовательной организацией. Результаты итоговой аттестации заносятся в соответствующие документы.

Итоговая аттестация проводится по форме представления учебных проектов и подготовки личного портфолио.

Промежуточная аттестация:

Практическая работа (выполнение заданий**):**

№п/п	***Тематика практического занятия***	***Форма ПА***
Модуль 1.	Технологии криптографии	Лабораторная работа
Модуль 2.	Защита «control plane»	Лабораторная работа
Модуль 3.	VPN удаленного доступа	Лабораторная работа
Модуль 4.	Зональный межсетевой экран CISCO IOS ZBF	Лабораторная работа
Модуль 5.	Безклиентский VPN удаленного доступа	Лабораторная работа
Модуль 6.	Расширенные архитектуры безопасности	Лабораторная работа

Итоговая аттестация по курсу (тестирование):

Вопросы теста/ответ:

«Сетевой уровень и маршрутизация»

101. Из-за чего возникает маршрутизация по кругу?
• После видоизменения сетевого комплекса имеет место низкая сходимость

102. Как сетевой уровень посылает пакеты от источника в пункт назначения?

• Используя таблицу IP-маршрутизации

103. Какая функция позволяет маршрутизаторам оценивать имеющиеся маршруты к пункту назначения и устанавливать предпочтительный способ обработки пакетов?
• Функция определения пути

104. Какие две части адреса используются маршрутизатором для передачи трафика по сети?
• Сетевой адрес и адрес хост-машины

105. Каково одно из преимуществ алгоритмов, основанных на использовании вектора расстояния?
• Просты в вычислении

106. Какое из приведенных ниже определений наилучшим образом описывает алгоритм маршрутизации с учетом состояния канала связи?
• Воссоздает точную топологию всего сетевого комплекса

107. Какое из приведенных ниже определений наилучшим образом описывает маршрутизируемый протокол?
• Обеспечивает достаточно информации, чтобы направить пакет от одной хост-машины к другой

108. Какое из приведенных ниже определений наилучшим образом описывает одну из функций уровня 3 (сетевого уровня) модели OSI?
• Определяет наилучший путь трафика через сеть

109. Какое из приведенных ниже определений наилучшим образом описывает протокол маршрутизации?
• Протокол, который выполняет маршрутизацию посредством реализованного в нем алгоритма

110. Какое из приведенных ниже определений наилучшим образом описывает сбалансированную гибридную маршрутизацию?
• Для определения наилучших путей в ней используются векторы расстояния, но обновления таблиц маршрутизации инициируются фактом изменения топологии

«Пользовательский интерфейс маршрутизатора и режимы»

111. Какие два режима доступа к командам маршрутизатора существуют в маршрутизаторах Cisco?
• Пользовательский и привилегированный

112. Какой из приведенных ниже символов свидетельствует о том, что данная командная строка является строкой привилегированного режима интерфейса пользователя маршрутизаторов Cisco?
• #

113. Какой из режимов предоставляет доступ к списку общеупотребительных команд, если при работе с интерфейсом пользователя маршрутизаторов Cisco ввести с клавиатуры символ знак вопроса ("?")?
• Пользовательский и привилегированный

114. Какой режим используется при внесении изменений в конфигурацию маршрутизаторов Cisco?
• Привилегированный

115. Нажатие каких клавиш при работе с интерфейсом пользователя маршрутизаторов Cisco приводит к автоматическому повторению ввода предыдущей команды?
• <Ctrl+P>

116. Что означает подсказка — More — , появляющаяся внизу экрана интерфейса пользователя

маршрутизаторов Cisco?
• Выводимая информация имеет несколько экранных страниц

117. Что означает, когда в интерфейсе пользователя маршрутизатора Cisco появляется символ "больше чем" (>)?
• Пользовательский режим

118. Что произойдет, если набрать команду show ? в командной строке?
• Будет показан перечень подкоманд, которые могут применяться совместно с командой show

119. Что произойдет, если при работе с интерфейсом пользователя маршрутизаторов Cisco ввести символ вопросительного знака?
• Пользователь войдет в систему помощи

120. Что произойдет, если при работе с интерфейсом пользователя маршрутизаторов Cisco нажать клавишу со стрелкой вверх?
• На экран будет выведена последняя введенная команда

«Вывод информации о конфигурации маршрутизатора»

121. Для чего используется команда show cdp neighbors?
• Для получения обзорной картины маршрутизаторов, непосредственно соединенных с сетью

122. Какая команда вводится для того, чтобы просмотреть файл активной конфигурации маршрутизатора?
• show running-config

123. Какие строки информации может выводить на экран команда show interfaces serial?
• Serial1 is up, line protocol is up

124. Какие четыре важных элемента информации получают после выдачи команды ping?
• Размер и количество ICMP-пакетов, продолжительность периода ожидания ответа, показатель успешности посылки эхо-пакетов и минимальное, среднее и максимальное время прохождения пакетов в оба конца

125. Какое из приведенных ниже определений описывает функцию команды show startup-config?
• Выводит сообщение, показывающее объем использованной энергонезависимой памяти

126. Какой из следующих компонентов маршрутизатора имеет такие характеристики: держит операционную систему и микрокод, сохраняет свое содержимое при отключении питания или перезапуске и позволяет обновлять программное обеспечение без замены микросхем?
• Флэш-память

127. Какую информацию дает проверка сети с помощью команды show interfaces serial?
• Показывает статус канала связи и канального протокола

128. Какую информацию дает проверка сети с помощью команды trace?
• Показывает каждый маршрутизатор, который проходит пакет на пути к пункту назначения

129. Что из приведенного ниже неправильно описывает функцию команды статуса маршрутизатора?
• show buffers выводит на экран статистические данные пулов буферов маршрутизатора

130. Что из приведенного ниже описывает место, из которого конфигурируется маршрутизатор?
• Будучи установленным в сеть, маршрутизатор может конфигурироваться с помощью

виртуальных терминалов

«Запуск маршрутизатора и его начальное конфигурирование»

131. Зачем может понадобиться выдача команд show startup-config и show running-oonfig?
• Маршрутизатор неожиданно начал неправильно работать, и необходимо сравнить начальное состояние с состоянием на данный момент времени

132. Какова функция команды erase startup-config?
• Удаляет из энергонезависимой памяти резервный конфигурационный файл

133. Какова функция команды reload?
• Перезагружает маршрутизатор

134. Какой (какие) файл (файлы) можно обнаружить в энергонезависимой памяти?
• Конфигурационные файлы

135. Когда выполняется режим начальной установки маршрутизатора?
• Когда маршрутизатор не может найти корректно оформленный конфигурационный файл

«Запуск маршрутизатора и его начальное конфигурирование»

136. Укажите правильную последовательность шагов выполнения процесса запуска системы маршрутизаторов Cisco:
1) тестирование аппаратной части
2) загрузка программы начального загрузчика
3) нахождение местоположения операционной системы и ее загрузка
4) нахождение местоположения конфигурационного файла и его загрузка

137. Что из приведенного ниже правильно описывает процедуру начальной установки на маршрутизаторе глобальных параметров и параметров интерфейсов?
• Должно быть установлено имя маршрутизатора

138. Что из приведенного ниже является важной функцией автопроверки по включению питания?
• Выполнение подпрограмм диагностики, которые проверяют принципиальную работоспособность аппаратной части маршрутизатора

139. Что из приведенного ниже является важным результатом ввода в маршрутизатор ОС IOS?
• Определение состава аппаратных и программных компонентов маршрутизатора и вывод этого перечня на терминал консоли

140. Что из приведенного ниже является важным результатом загрузки в маршрутизатор конфигурационного файла?
• Запуск процесса маршрутизации, ввод адресов интерфейсов и установка характеристик сред передачи данных

«Конфигурирование маршрутизатора»

141. Если необходимо выйти из режима конфигурирования, то какую из следующих команд следует ввести?
• <Ctrl+Z>

142. Если планируется конфигурирование интерфейса, то какой вид должна иметь командная строка маршрутизатора?
• Router(config-if)#

143. Какая из следующих команд не является командой удаления изменений в конфигурации маршрутизатора?
• Router# copy running-config startup-config

144. Какова функция команды configure memory?
• Выполняет загрузку конфигурационной информации из энергонезависимой памяти

145. Какова функция команды copy running-config startup-config?
• Сохраняет в энергонезависимой памяти текущую конфигурацию, находящуюся в ОЗУ

146. Какую из приведенных ниже команд можно использовать для сохранения изменений конфигурации маршрутизатора в резервной копии конфигурационного файла?
• Router# copy running-config tftp

147. Укажите правильный порядок процесса конфигурирования маршрутизатора: (Предполагается, что изменения в маршрутизаторе с помощью режима конфигурирования уже были сделаны.)
1) Проверка результатов
2) Принятие решения относительного того, являются ли изменения желаемым результатом
3) Сохранение изменений в резервной копии
4) Проверка резервного файла

148. Что из приведенного ниже не описывает процедуру конфигурирования пароля в маршрутизаторах?
• Пароли могут устанавливаться при работе в любом режиме конфигурирования

149. Что из приведенного ниже не является функцией команды привилегированного режима EXEC configure?
• Конфигурирование TFTP-сервера с виртуального терминала

150. Что из приведенного ниже правильно описывает конфигурирование в маршрутизаторе паролей?
• Пароль может быть установлен на все входящие сеансы протокола Telnet

«Источники загрузки ОС IOS»

151. Для чего необходимо определять размер файла образа ОС IOS на TFTP-сервере перед пересылкой его в маршрутизатор?
• Чтобы проверить достаточность пространства во флэш-памяти для его сохранения

152. Зачем создается резервная копия образа ОС IOS?
• Для создания аварийной копии текущего образа перед переходом на новую версию

153. Какой способ является самым быстрым для проверки достижимости TFTP-сервера перед попыткой пересылки файла образа ОС IOS?
• Пропинговать TFTP-сервер с помощью команды ping

154. Какую команду следует выдать, если необходимо обновить старую версию ОС IOS путем загрузки нового образа с TFTP-сервера?
• copy tftp flash***

155. Укажите последовательность, используемую маршрутизатором, для автоматического возврата в исходное состояние и обнаружения местонахождения источника ОС IOS:
1) Энергонезависимое ЗУ
2) Флэш-память
3) TFTP-сервер

156. Что из приведенного ниже выводится на экран командой ОС IOS show version:
• Версия ОС IOS
• Тип платформы, на которой исполняется ОС
• Установка регистра конфигурирования

157. Что из приведенного ниже не описывает установки регистра конфигурирования для начальной загрузки ОС IOS?
• Для проверки установки поля начальной загрузки используется команда show running-config

158. Что из приведенного ниже не является частью процесса задания аварийной последовательности для начальной загрузки ОС IOS?
• Для задания всей аварийной последовательности используется одна команда начальной загрузки системы

159. Что из приведенного ниже правильно описывает подготовку к использованию TFTP-сервера для копирования программного обеспечения во флэш-память?
• TFTP-сервер должен быть другим маршрутизатором или хост-системой, например рабочей станцией с ОС UNIX или портативным компьютером

160. Что, по-вашему, содержит ограниченную версию ОС IOS?
• ПЗУ

«Конфигурирование IP-адресов интерфейсов маршрутизатора»

161. Если необходимо отобразить имя домена на IP-адрес, то что надо сделать сначала?
• Идентифицировать имена хост-машин

162. Какова функция команды ping?
• Использует протокол ICMP для проверки возможности соединения на физическом уровне и логического адреса сетевого уровня

163. Какова функция команды telnet?
• Проверяет работоспособность программного обеспечения уровня приложений на участке между станцией-отправителем и станцией-получателем

164. Какова цель использования команды trace?
• Она локализует отказы по пути от отправителя к получателю

165. Каково назначение команды ip name-server?
• Задает хост-машины, которые могут предоставить сервис работы с именами

«Конфигурирование IP-адресов интерфейсов маршрутизатора»

166. Каково назначение команды no ip domain-lookup?
• Отключает в маршрутизаторе функцию преобразования "имя—адрес"

167. Какую команду следует использовать для занесения статической записи отображения "имя—адрес" в конфигурационный файл маршрутизатора?
• ip host

168. Что из приведенного ниже наилучшим образом описывает функцию адреса широковещания?
• Посылает сообщение всем узлам в сети

169. Что из приведенного ниже наилучшим образом описывает функцию команды show hosts?
• Используется для вывода на экран находящегося в кэше списка имен и адресов

170. Что из приведенного ниже наилучшим образом описывает функцию расширенной команды ping?
• Используется для задания поддерживаемых в сети Internet-заголовков

«Конфигурирование маршрутизатора, RIP и IGRP»

171. Для чего выводится содержимое таблицы IP-маршрутизации?
• Для идентификации пар значений адресов сетей назначений и количества переходов

172. Для чего используются протоколы внешней маршрутизации?
• Для обмена информацией между автономными системами

173. Для чего используются протоколы внутренней маршрутизации?
• Используются внутри одной автономной системы

174. Если необходимо узнать, на работу с каким протоколом маршрутизации сконфигурирован маршрутизатор, то какую команду следует использовать?
• Router> show ip protocol

175. Есть подозрение, что один из маршрутизаторов в сети посылает плохую маршрутную информацию. Какую команду можно использовать для проверки?
• Router> show ip protocol

176. К какому типу записей маршрутизатор обращается первоначально?
• К записям о сетях и подсетях, подключенных непосредственно

177. Какую метрику использует протокол RIP для определения наилучшего пути, которым должно следовать сообщение?
• Количество переходов

178. Что из приведенного ниже наилучшим образом описывает маршрут по умолчанию?
• Запись в таблице маршрутизации, которая используется для направления кадров, следующий переход для которых не имеет явного отражения в таблице маршрутизации

179. Что из приведенного ниже наилучшим образом описывает статический маршрут?
• Маршрут, который в явном виде конфигурируется и вводится в таблицу маршрутизации и имеет преимущество над маршрутами, выбранными протоколами динамической маршрутизации

180. Что из приведенного ниже относится к задачам глобального конфигурирования?
• Выбор протокола маршрутизации: RIP или IGRP

«Управление сетью»

181. Какие шаги следует предпринять для анализа и решения проблемы в сети после сбора данных о работе?
• Составить список возможных причин; расставить приоритеты причин; используя средства управления сетью или метод замены, идентифицировать причины

182. Каким образом карта сети помогает локализовать место возникновения проблемы с физическим элементом сети?
• Предоставляет информацию об адресах проблемного устройства

183. Какова цель инвентаризационной ревизии?
• Составление инвентаризационной описи всего программного и аппаратного обеспечения, используемого в сети

184. Какова цель ревизии средств защиты сети?
• Определение состава аппаратно-программного комплекса, требующегося для обеспечения защиты сети

185. Какова цель ревизии установленного оборудования?
• Идентификация местонахождения каждого элемента сети

186. Какова цель ревизии эффективности?
• Определение того, работает ли сеть в соответствии со своим потенциалом

187. Что должно входить в письменную форму документа "Технические требования на изменения", который готовится для достижения более высокой производительности и уровня защиты сети?
• Обоснования каждого запрашиваемого изменения

188. Что из приведенного ниже должно быть включено в отчет о проведении оценки?
• Журналы, показывающие тенденцию к уменьшению скорости трафика в определенных сегментах сети

189. Что из приведенного ниже правильно описывает протокол SNMP?
• Использует концепцию, известную под названием MIB

190. Что из приведенного ниже правильно описывает работу протокола CMIP?
• Предусматривает наличие центральной рабочей станции мониторинга, которая ожидает от устройств сообщений об их текущем состоянии

«Эталонная модель OSI и маршрутизация»

191. В случае, когда все маршрутизаторы в сети работают с одной и той же информацией о топологии сети, то о сети говорят как о...
• конвергированной

192. Какая из следующих функций используется маршрутизатором для пересылки пакетов данных между сетями?
• Определение пути и коммутация

193. Какие из перечисленных ниже являются основными типами динамической маршрутизации?
• Дистанционно-векторный и канальный

194. Какое из приведенных ниже утверждений наилучшим образом описывает функции транспортного уровня эталонной модели OSI?
• Он посылает данные, используя управление потоком

195. Какой уровень эталонной модели OSI наилучшим образом описывает стандарты 10BaseT?
• Физический

«Коммутация в локальных сетях»

196. Для чего оптимизируется асимметричная коммутация?
• Для потока данных сети в случае, когда "быстрый" порт коммутатора подсоединен к серверу

197. Каково минимальное время, требуемое для передачи одного байта данных в сети Ethernet?
• 800 наносекунд

198. Какой из приведенных ниже методов широковещания используется передающей средой Ethernet для передачи и получения данных от всех узлов сети?

• Фреймы данных

199. Коммутаторами Ethernet являются...
• Мосты с несколькими портами на 2 уровне

200. При _____ коммутации коммутатор проверяет адрес получателя и сразу начинает отправку пакета, а при _____ коммутации коммутатор получает фрейм полностью перед последующей его отправкой.
• Сквозной; с промежуточным хранением

201. Протокол распределенного связующего дерева позволяет...
• использовать дополнительные пути, без отрицательных эффектов от образования петель

202. Что из перечисленного ниже характеризует микросегментацию сети?
• Выделенные пути между хостами отправителя и получателя
• Несколько путей передачи данных внутри коммутатора

«Виртуальные локальные сети»

203. Каждый сегмент _____, подсоединенный к порту _____, может быть назначен только одной виртуальной сети.
• Концентратора; коммутатора

204. Коммутаторы, которые являются ключевым элементом виртуальных сетей, дают возможность выполнить следующее:
• Выполнять обмен информацией между коммутаторами и маршрутизаторами
• Принять решения о фильтрации и отправке фреймов
• Сгруппировать пользователей, порты или логические адреса в виртуальной сети

205. Термин расширяемая микросегментация означает следующее:
• Возможность расширения сети без создания коллизионных доменов

206. Что из перечисленного ниже не является достоинством статической виртуальной сети?
• Автоматическое обновление конфигурации портов при добавлении новых станций

207. Что из перечисленного ниже не является характерным признаком виртуальной сети?
• Все перечисленные понятия являются характерными признаками виртуальной сети

208. Что из перечисленного ниже является положительным результатом использования виртуальной сети?
• Отсутствует необходимость конфигурирования коммутаторов

«Проектирование локальных сетей»

209. Какая из следующих характеристик не верна для 10BaseT?
• Максимальная длина — 400 метров

210. Основная цель проектирования канального уровня — это выбор устройств _____, таких как мосты или коммутаторы локальных сетей, используемых для соединения носителей _____ с целью образования сегментов локальных сетей?
• 2-го уровня; 1-го уровня

«Проектирование локальных сетей»

211. Что из перечисленного ниже вероятнее всего вызовет перегрузку в сети?
• Доступ в Internet

• Доступ к главной базе данных
• Передача графики и видео

212. Что из перечисленного ниже не вызывает чрезмерного широковещания?
• Слишком много сетевых сегментов

213. Что является преимуществом использования устройств 3-го уровня в локальной сети?
• Оно обеспечивает логическое структурирование сети
• Оно позволяет разделять локальную сеть на уникальные физические и логические сети
• Оно фильтрует широковещание и многоадресные рассылки канального уровня и позволяют подключаться к распределенным сетям

«Протоколы маршрутизации IGRP»

214. _____ протоколы маршрутизации определяют направление и расстояние до любого канала сети совместного использования; _____ протоколы маршрутизации также называются протоколами выбора первого кратчайшего пути.
• Дистанционно-векторные; канального уровня

215. Какую из приведенных ниже команд следует использовать для выбора IGRP в качестве протокола маршрутизации?
• router igrp

216. От какого из приведенных ниже действий зависит успех динамической маршрутизации?
• Периодическое внесение изменений в таблицу маршрутизации
• Поддержание таблицы маршрутизации

217. После определения пути, по которому следует направить пакет, какое следующее действие может выполнить маршрутизатор?
• Коммутация пакета

218. Что из перечисленного ниже не является переменной, используемой протоколом IGRP для определения значения комбинированной метрики?
• Протокол IGRP использует все эти величины

«Списки управления доступом (ACL)»

219. Как называются дополнительные 32 бита в директиве access-list?
• Биты шаблона

220. Каким образом маршрутизатор различает стандартные списки управления доступом и расширенные?
• Стандартные списки управления доступом имеют номера от 1 до 99. Расширенные списки управления доступом имеют номера от 100 до 199

221. Какому из приведенных ниже высказываний эквивалентно выполнение команды Router(config)# access-list 1 156.1.0.0 0.0.255.255?
• "Разрешить доступ только к моей сети."

222. Какую из приведенных ниже команд следует использовать для того, чтобы выяснить, установлены ли на данном интерфейсе списки управления доступом?
• show ip interface

223. Команда show access-list используется для того, чтобы:
• просмотреть директивы списка управления доступом

224. Утверждение: "При задании разрешения на доступ в списке управления, сопровождаемом неявным "отказать всем", всем потокам данных, кроме указанного в директиве permit, будет отказано в доступе".
• Истинно